DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

February 6 - March 4, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071460	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	2/6/2012		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0546954	2/6/2012	INC000000196338	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

02/06/12:
Patient B will be sent a notification letter.

NOTE: There were a total of 5 Mis-Mailed CMOP incidents out of 6,279,359 total packages (9,234,400 total prescriptions) mailed out for this reporting period. Because of repetition, the other 4 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071634	Missing/Stolen Equipment	VISN 23 Omaha, NE	2/9/2012		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0547866	2/9/2012	INC000000197266	N/A	N/A	N/A		

Incident Summary

At approximately 9:00 AM on 02/09/12 an Omaha PC technician received a trouble ticket that a desktop PC at the Bellevue NE Community Based Outpatient Clinic (CBOC) would not boot up and was displaying an error message consistent with a failed hard drive. He went onsite to replace the CPU tower and returned the old one to the main hospital facility. When he opened the computer tower, he discovered that the internal hard drive was missing.

Incident Update

02/10/12:
The PC technician determined that this hard drive was installed in and successfully operating from another PC in the Bellevue CBOC. He is now attempting to locate the hard drive that should have been in this second PC, first by searching the history of work tickets for that facility. There has been no sign of an internal hard drive laying around in the Bellevue CBOC. This second hard drive was also installed in an exam room.

03/06/12:
The PC technicians are still searching for the second hard drive. They have checked their ticket system but have not found any indication of work on the second PC involving the hard drive. They have also checked with the vendor to see if any warranty work was done on the second PC with negative results.

03/06/12:
The PC technicians found a hard drive in their office which is consistent with the make and model that would have come out of the PC in question. They attempted to connect to it to determine which PC it came from, but they were not successful. They are preparing to ship the hard drive to the NSOC for forensic examination to determine which computer this hard drive came from.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071714	Mishandled/ Misused Physical or Verbal Information	VISN 18 El Paso, TX	2/13/2012		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0548383	2/13/2012	INC000000197741	N/A	N/A	N/A	1	

Incident Summary

Veteran A called the Privacy Officer (PO) to report the receipt of an envelope with 2 pages containing Veteran B's registration information via USPS mail delivery. He stated that he would return the entire letter, envelope and 2 pages of information to the Community Based Outpatient Clinic (CBOC) Manager for return to the facility. Veteran A expressed concern about the mis-mailing to him of Veteran B's private information and wanted to make sure the problem would be addressed. The packet was received in the Privacy Office that included 2 pages of registration information/demographics on Veteran B including full name, full social security number, date of birth, home and cell phone numbers, co-pay, and name of provider, future appointments, home address, and name of spouse.

Incident Update

02/13/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 97 Mis-Mailed incidents this reporting period. Because of repetition, the other 96 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071734	Mishandled/ Misused Physical or Verbal Information	VISN 18 Big Spring, TX	2/13/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0548468	2/13/2012	INC000000197860	N/A	N/A	N/A	408	3

Incident Summary

On 02/10/12, Big Springs, TX VAMC shipped 65 boxes on two pallets to the Records Center & Vault (RC&V) in Neosho, Missouri. Yellow Freight delivered them on 02/13/12. The boxes contained medical files. Upon delivery the RC&V staff noticed there were only 64 boxes on the pallets. The RC&V Archives Technician called the Big Springs Point of Contact (POC) who confirmed that there were 65 boxes on the pallets when they were picked up from Big Springs. The missing box was stacked on the very top of pallet two. The shrink wrap was loose in the spot where the box was at one point. The RC&V contacted the VA Transportation office and informed them of the missing box. Yellow Freight provided a tracking number. The Big Springs POC stated the missing box contained eight files for three Veterans in addition to the entire inventory for all 65 boxes. The inventory consists of the full name, Social Security number, and chart number.

Incident Update

02/21/12:
The facility Privacy Officer (PO) and facility Logistics have a ticket into Yellow Freight to locate the missing box. As of 02/21/12, Yellow Freight has not been able to locate the missing box.

02/27/12:
The facility is awaiting a response from Yellow Freight. The timeframe Yellow Freight allows for searching for a missing item has not lapsed.

03/08/12:
Yellow Freight has not located the missing box.

03/13/12:
The Data Breach Core Team (DBCT) has determined to move ahead with credit protection service letters and next-of-kin notifications due to the length of time the shipping company has been looking for the missing box. Four-hundred and eight Veterans will receive letters offering credit protection services and three next-of-kin notifications will be sent.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071811	Mishandled/ Misused Physical or Verbal Information	VISN 04 Lebanon, PA	2/15/2012	2/27/2012	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0548953	2/15/2012	INC000000198236	N/A	N/A	N/A		1

Incident Summary

Patient A came to the Pharmacy window to pick up his prescriptions. The Pharmacy technician verified Patient A's ID and reviewed the medications, but when retrieving the bag of medications, the Pharmacy technician pulled out a bag of medications for Patient B and scanned them out of the system. Shortly after leaving the Pharmacy, Patient A realized he had the incorrect bag of medications and returned the bag of medications to the Pharmacy. Patient B's name, address and type of medication were compromised.

Incident Update

02/15/12:
Patient B will be sent a notification letter.

NOTE: There were a total of 92 Mis-Handling incidents this reporting period. Because of repetition, the other 91 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The Pharmacy technician was reminded of the importance of ensuring that the correct patient gets the correct medications.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072242	Mishandled/ Misused Physical or Verbal Information	VISN 18 Phoenix, AZ	2/28/2012	3/13/2012	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0551631	2/28/2012	INC000000200211	N/A	Yes	N/A		1

Incident Summary

Today at 11:15 AM, the Women's Program Manager notified the Privacy Officer (PO) of a privacy event involving Veteran B. The PO was told that Veteran B left the VA with Veteran A's appointment schedule. This appointment schedule was previously provided to Veteran B on 12/15/2011 by another clinic. Today, when Veteran B went to this clinic for an appointment, they informed her that no appointment for her was scheduled. They reviewed the document that she had with her which turned out to be the scheduling sheet of Veteran A. The clinic staff accommodated Veteran B with an appointment slot but did not recover the document. The Patient Advocate and the Women's Program Manager were notified.

The Women's Program Manager instructed Veteran B to relinquish Veteran A's schedule which was refused. Veteran A's information on the scheduling sheet included only first name, last name and last 4 digits of the SSN. There was no diagnosis, address or other contact information. Veteran A ran from Women's Program Office with materials before the PO could arrive. The VA Police were notified. There is a low indication of theft based on what VA provided to her in error. However, the documents were requested back to protect other Veteran which Veteran B refused to do.

Incident Update

02/28/12:
Veteran A will be sent a notification letter.

03/01/12:
Veteran B who has the information has still not returned the information, and is posting information about what the VA has done on Facebook, Twitter, and the local press. The VA Police have been unsuccessful in getting the VA information back on Veteran A.

Resolution

The Outpatient Chief discussed and counseled the employee involved in the incident. Disciplinary action is being reviewed. A HIPAA notification and complaint response were drafted for Regional Counsel's review. The letters to both Veterans A & B were signed by the Director and mailed to them.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072346	Mishandled/ Misused Physical or Verbal Information	VISN 07 Tuscaloosa, AL	3/1/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0552148	3/1/2012	INC000000200652	3/1/2012	Yes	Pending		

Incident Summary

On 02/29/12, the Privacy Officer (PO) was notified by a Logistics Property Specialist that sensitive patient information was discovered in Building 38, in the 1st Floor construction area. The Specialist stated that she went to conduct an equipment inventory listing (EIL) audit for equipment possibly located in Building 38. During her search for the missing VA equipment, she asked a construction worker if he noticed any VA equipment in his construction area. The construction worker proceeded to show the Specialist the equipment, medical supplies and a stack of papers on the floor where the movers unloaded a credenza leaving the papers, etc. on the floor. The Specialist informed the PO that there are a stack of papers and VA equipment consisting of phlebotomy logs containing full name, last 4 digits of the SSN and clinic number, flu vaccine completed forms containing full name, last 4 digits of the SSN, some with vitals taken by nursing staff, the name of the Primary Care provider and allergies, an old IT printer, medical supplies, two sharps containers and a blood draw chair.

Incident Update

03/05/12:
The papers were removed from a credenza by movers when they removed the furniture from the room on 01/11/12 or 01/12/12. The area was under construction and the only people known to be in the area are construction workers, however the area was not locked.

03/-6/12:
The construction site is part of an outpatient clinic within the medical center. The clinic is still accepting patients so there is constant traffic consisting of employees, patients and visitors near the construction site. The area is closed off with heavy construction plastic and to enter the area, one would have to go through two small entrances. It is unlikely that anyone who did not belong in the construction site entered the area.

03/13/12:
The Data Breach Core Team (DBCT) reviewed this incident and determined that the risk of exposure was very minimal. No breach has occurred.

NOTE: There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072371	Unauthorized Electronic Access	VISN 04 Pittsburgh, PA	3/1/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0552252	3/1/2012	INC000000200736	N/A	N/A	N/A	60	

Incident Summary

The Privacy Officer (PO) was notified that VA residents have been requesting Veteran imaging CDs for presentation purposes. The Imaging Supervisor indicated this activity has been occurring for the last few years. The imaging clerks have been providing the VA residents with VA Form 0897 (Presenter Certification Form), VHA Privacy Office Privacy Fact sheet volume 08, No.2 (Displaying Sensitive Information in Presentations) and an unencrypted CD of the requested images. The residents signed VA Form 10-5345 (Request For and Authorization to Release Medical Records) however this is not the appropriate signature authority for presentation purposes. The signed VA Form 0897 and presentations have not been submitted to the Privacy Office for review.

Incident Update

03/01/12:
This process was stopped immediately. The PO requested to see documentation of all images released under these circumstances in the past year as an auditing measure. The PO received approximately 40 for fiscal year 2011; in which none had been submitted to the Privacy Office for review. The Imaging Supervisor has been asked to provide copies of all VA Form 10-5345 that have been signed by the resident/physicians for these purposes. The images contained full name, SSN, age, sex, date of birth, referring physician, type of exam and date of exam.

03/06/12:
These requests should not have been a FOIA request as all the Veterans are still living. The presentations were all for educational purposes, presented at educational conferences, review cases, case conferences, surgery and peri-operative care, etc.. With the Veterans still living, the approving authority would have been the Veteran him/herself. The PO identified a total of 60 Veterans.

03/13/12:
Although no malicious intent was involved, the personally identifiable information (PII) for 60 Veterans was inappropriately disclosed. Letters offering credit protection services will be sent to all 60 Veterans.

Resolution

OI&T staff assisted the Imaging Department with implementing the redaction capability on the imaging software. The Imaging Department will only provide a de-identified encrypted CD for presentation purposes after a request has been received in writing. In addition, the Imaging Department will track these disclosures and notify the Privacy Office.

Total number of Internal Un-encrypted E-mail Incidents	113
Total number of Mis-Handling Incidents	92
Total number of Mis-Mailed Incidents	97
Total number of Mis-Mailed CMOP Incidents	5
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	0
Total number of Missing/Stolen Laptop Incidents	9 (8 encrypted)
Total number of Lost BlackBerry Incidents	21
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0